Chapter 10

Rear Battle

10-1. General

a. To provide continuous effective communications at EAC, the TACSAT Company must be able to survive in a hostile environment. A major aspect of enemy doctrine is to disrupt rear area operations. When CPs and communications nodes are located, the enemy will try to neutralize them. Detection must be avoided to survive. Also, it may be necessary to defend terminal sites. Successful self-defense requires planning, preparing, rehearsing, and virgorous execution.

b. The TACSAT Company commander must prepare personnel for defense. Plans are based on coordination with supported units. This chapter will highlight the various types of threats to the TACSAT Company. It will then emphasize defensive considerations. Because the subject is too broad and technical to cover completely, reference will be made to appropriate manuals to consult for details. Also, soldier's manuals (SM) for the senior skill levels within the TACSAT Company list many of the tasks to be performed for specific security and defense situations.

10-2. Rear battle threat

a. The rear area is the space within a command where the majority of the combat support and combat service support functions are peformed. In a fully developed theater of operations, the whole COMMZ is classed as rear area. The enemy has the capability to initiate and support combat operations deep in the COMMZ. Their objective is to destroy critical elements, cause disruption, and degrade capabilities. The TACSAT Company is usually employed in the COMMZ but may also be employed in the rear of the combat zone.

b. The enemy threat to rear battle opertions may be of low, medium, or high intensity. These three levels of threat are summarized in table 10-1. Commanders develop alert systems and response actions according to the level of threat that must be countered. Elements of the TACSAT Company may face any combination of enemy forces at the same time. Other disruptive occurrences include conventional and NBC shelling and bombing and natural disasters.

Table 10-1. Rear battle threat levels and responses

Threat Level	Threat	Response Forces
Level I	Agents, saboteurs, terrorists	Base defense
Level II	Diversionary operations and sabotage by unconventional and reconnaissance forces, raids by tactical units, special or unconventional warfare missions	Military police (base defense)
Level III	Airborne, heliborne, amphibious, and ground forces deliberate operations, infiltration operations	Tactical combat forces (military police) (base defense)

10-3. Unit security and defense

a. General. TACSAT Company security and defense is accomplished within guidelines established by U.S. Army rear battle doctrine. The rear battle is designed to make collective use of units in the rear area to prevent or minimize interruption of operations. It includes measures taken to protect the resources of rear area commands against sabotage, enemy activity, and natural disasters. Rear battle objectives include the following:

(1) Secure the rear area and facilities.

(2) Prevent or minimize enemy interference with command, control, and communications.

(3) Prevent or minimize disruption of combat support and combat service support forward.

(4) Provide unimpeded movement of friendly units throughout the rear area.

(5) Find, the, and destroy enemy intrusions in the rear area.

(6) Provide area damage control (ADC).

b. Rear battle command and control. The TA commander is responsible for rear battle planning and execution at EAC. Rear battle operations are conducted through decentralized command and control systems used by EAC rear area operations centers (RAOCs). RAOCs are usually established at TA, TAACOM, and TAACOM area support group (ASG) levels. Each echelon commander will appoint a rear battle officer to conduct rear battle operations. Where HNS agreements have been reached, certain rear battle responsibilities may be assumed by the host nation. Within a TAACOM, TACSAT elements would be assigned to particular bases for defense purposes. The base commander provides the command and control headquarters for base defense. The base defense operations center (BDOC) is staffed and equipped by the host and tenant units. Sometimes, base clusters are formed for mutual defense and controlled through a base cluster operation center (BCOC). TACSAT elements plan for the defense of of their sites as part of base defense. Terminal section chiefs submit plans to the BDOC for approval. Defense plans should also include ADC considerations. See FM 90-14 for complete details on rear battle command and control.

c. Conduct of the rear battle. Responses to enemy attacks in the rear area must be rapid and strong enough to defeat the enemy. They must minimize disruption of friendly operations. Table 10-1 also shows rear battle responses to the various threat levels. Obviously, base defense is the cornerstrone for effective conduct of the rear battle.

d. Unit defense planning. Detailed planning is done by the dispersed TACSAT sections per unit SOP. Frequently, TACSAT Company assets will be deployed to remote locations. Site defense planning should be as complete as possible but flexible. One cannot plan for every situation. Defense or security requirements beyond organic capability should be identified. When unable to defeat attacking forces, site defense forces attempt to defend the site or base until other forces can respond. Defense procedures should be simple and easy to implement. Individual responsibilities should be clearly defined. One basic plan with alternative courses of action for meeting various threats is probably best.

e. Defense against air and ground attack.

(1) TACSAT terminal sections have a distinctive signature. They must rely heavily on sound (OPSEC). This includes taking all counter reconnaissance and surveillance actions (for example, camouflage, watching thermal signature, controlling electronic emissions, and so forth). Facilities should be camouflaged, concealed, covered, and dispersed as much as possible (FM 5-20). Warnings against air attack are broadcast over the air warning net which should be constantly monitored. Army counterintelligence (CI) also can provide early warning and recommend OPSEC procedures to counter enemy intrusions into the rear area (FM 34-60). Defense against ground attack should be based on a sound site defense plan. Some actions to be taken in most defensive situations are listed below:

(a) Assign sectors of defense.

(b) Locate a focal point for command and control.

(c) Ensure individuals are familiar with their responsibilities.

(d) Prepare positions (FM 5-15).

(e) Place weapons to cover avenues of approach.

(f) Use artificial obstacles and mines as required.

(g) Coordinator with adjacent units.

(h) Hold frequent rehearsals and inspections.

(i) Practice camouflage, light, and noise discipline.

(j) Design a warning system.

(k) Establish procedures for requesting artillery and air support.

(l) Designate assembly points for reserve forces and fire fighting crews.

(m) Plan for the evacuation of casualities.

(n) Plan for the destruction of equipment and supplies.

(2) Personnel are trained in the use of their individual weapons and in defensive measures, but have a limited capability to defend themselves. The TACSAT Company commander should schedule refresher training and conduct defense exercises.

f. Area damage control. The TACSAT Company must plan and train for ADC operations. ADC limits damage, seals off affected areas, salvages equipment, saves lives, and restores operations. ADC activities should be included in SOPs and rehearsed to ensure individuals are certain of their responsibilities (FM 90-14). In most cases, the dispersed TACSAT elements should incorporate their ADC measures with those of collocated units.

1O-4 Emergency destruction of equipment

a. Emergency destruction (ED) is a command responsibility. Sensitive equipment and cryptomaterial are involved in all TACSAT units. Due to the lack of mobility of the terminal sections, ED is a distinct possibility. The TACSAT Company SOP must include ED plans. Plans should be simple, capable of rapid execution, and should include priorities and methods for destruction. Specific people

must be designated to perform the destruction. Common methods of destruction include smashing, cutting, burning, bending, breaking, burying, and scattering. If explosives are required, people must be trained to use them. See appropriate TMs for destruction procedures.

b. Proper authorization for ED is required. ED is usually ordered by higher commanders as a last resort. The SOP should be specific as to what constitutes a local decision to destroy equipment. When ED is accomplished, a report should be made to higher headquarters. For more detail on ED of equipment, see AR 380–5 and FM 5–25.

10–5. Nuclear, biological, and chemical threat

A coordinated enemy attack of the COMMZ may well include NBC warfare. Few munitions can disrupt operations as extensively as NBC. The effects cover large areas. They are capable of causing enormous destruction and massive casualties. Communications centers and nodes will likely be prime targets. The purpose of this section is to acquaint TACSAT Company personnel with the severity of the threat posed by NBC munitions. You can consult FM 3-100 for more complete information on the effects of NBC warfare.

a. Nuclear weapon effects. There are five main effects from a nuclear detonation: blast, thermal radiation, nuclear radiation, electromagnetic pulse (EMP), and nuclear blackout. Aside from the obvious devastating effects of a nuclear explosion, C-E systems are extremely susceptible to EMP and blackout.

(1) *Blast.* Blast causes most of the destruction created by a nuclear detonation. Exposed troops can be crushed by the overpressures or injured by flying debris. Personnel inside structures can be injured by their collapse.

(2) *Thermal radiation.* Immediate intense heat starts fires in buildings and forests. The heat can also burn exposed skin at distances where blast and nuclear radiation effects are minor. The extremely bright light formed can cause temporary or permanent blindness.

(3) *Nuclear radiation.* Initial nuclear radiation is emitted within the first minute after detonation. To survive initial radiation, personnel must be in a protected position before the detonation. Residual radiation lasts after the first minute. It consists of fallout or neutron-induced radiation near the point of detonation. Fallout is the primary residual hazard. Electronic systems are also sensitive to nuclear radiation effects.

(4) *Electromagnetic pulse.* EMP is a short duration radio frequency pulse. EMP does not affect personnel. However, radio and TACSAT equipment can be damaged or made inoperative by EMP. Unless well buried, cable and wire will pick up EMP energy which is higher than the circuit and component capabilities of the equipment. The damage can range from burned out fuses, transistors, and coils to the destruction of complete power supplies. Table 10-2 provides an indication of the vulnerability of tactical equipment to EMP.

(5) *Nuclear blackout.* Nuclear blackout is the result of the fireball itself and the large dust clouds which may be created. It can last from a few seconds to many hours. It affects radio and TACSAT communications by—

(a) Refraction (bending of the waves).

(b) Absorption (consuming the waves).

(c) Scattering (scattering the waves in all directions).

b. Biological agent effects. Biological agents consist of disease-producing germs and toxins. These agents may be dispersed as aerosols by generators, explosives, shells, missiles, and aircraft. The aerosol form allows them to be spread rapidly by the wind and cover large areas. Harmful germs may also be spread by the release of infected insects. Germs and toxins can be used to cause injury, death, and disease among humans, animals, and plants. They also can be used to cause deterioration of materials and contaminate supplies. Anti-personnel biological agents have little affect on electronic components. However, C-E equipment may require decontamination in order to eliminate persistent contact hazards.

c. *Chemical agent effects.*

(1) Chemical agents are a significant threat to TACSAT Company personnel as well as to equipment. They can be disseminated by aircraft, artillery, rockets, and missiles. The severity of the effect is dependent upon the dose received. Chemical agents fall into four classes:

(a) Nerve agents that directly affect the nervous system.

(b) Blister agents that affect the eyes and lungs and blister the skin.

(c) Blood agents that affect the circulatory and respiratory systems by preventing the body's cells from using oxygen.

(d) Choking agents that affect the respiratory system by attacking the lungs.

(2) Persistent chemical agents may contaminate supplies and equipment and restrict the use of terrain and facilities for hours and days.

Table 10-2. Equipment vulnerability to EMP

Equipment Categories	Probability of Damage	Equipment Included in Category
I	Very low	Artillery, tactical equipment (excluding communications equipment).
II	Low	Fire direction control equipment, nuclear warheads, missiles.
III	Medium	Long-range communications equipment (greater than 100 km), air defense radars.
IV	High	Target acquisition radars, short-range communications equipment (less than 100 km), command and control equipment.

10-6. Nuclear, biological, and chemical defense

The TACSAT Company must be prepared to function under NBC conditions. FM 11-23 directs every TCC(A) unit to become proficient in the survival techniques and operational standards for NBC warfare. NBC defense must be fully integrated into unit planning and training programs.

a. Defense tasks and planning.

(1) The TACSAT Company must plan for three basic NBC defense tasks discussed in *(a)* through *(c)* below. The successful performance of these tasks should be the objective of the TACSAT Company NBC training program.

(a) Contamination avoidance. Contamination avoidance is accomplished through NBC awareness, detection and warning of NBC hazards, and limiting the spread of contamination. Contaminated areas should be bypassed if possible. If not, personnel must use protective clothing and equipment. FM 3-3, chapter 2, covers the marking of contaminated areas.

(b) Protection of Personnel. Personnel must be protected to maintain the integrity of TACSAT operations. During the threat of an NBC attack, the TACSAT Company commander can balance personnel safety with unit effectiveness by using a mission-oriented protective posture (MOPP). The MOPP prescribes what clothing and equipment must be worn and/or used and what operational precautionary measures must be applied. Table 10-3 shows example requirements for protective clothing and equipment for different MOPP levels. FM 3-100 must be consulted for the detail necessary to prepare MOPP levels appropriate to the TACSAT Company. FM 3-3 provides added detail to prepare nuclear MOPP levels. All MOPP information should be placed in the TACSAT Company SOP. Protective clothing and equipment should be carried at all times. Also, see FM 3-4 for NBC protection procedures.

(c) Decontamination. Decontamination reduces casualties and improves individual and unit effectiveness. Individuals must be trained to perform emergency self-decontamination. Units must have the capability to perform personnel decontamination and partial equipment decontamination. The source of decontamination devices and trained specialists should be determined. FM 3-5 provides a guide for NBC decontamination.

(2) The NBC plan can be part of the unit defense plan or an annex to it. Dispersed TACSAT elements must be integrated into the supported unit NBC plan. For the details needed to plan and train for NBC defense, see FM 3-100. As indicated, unit SOP for defense against NBC is a requirement.

(3) The TACSAT Company's NBC program is directed by the chemical NCO. An NBC control party is formed to plan and conduct unit NBC defense. Other teams should be designated as required. Each element of the TACSAT Company must be made aware of its responsibilities for NBC defense.

b. Decontamination of communications equipment. Decontamination of TACSAT Company equipment must be done very carefully. Ensure the power supply is disconnected to prevent injury to personnel and damage to the equipment. FM 3-5 provides instructions for the decontamination of metal, plastic, leather, and wood parts. Crae must be taken not to damage electronic components with decontamination solutions. Some decontaminants, by their nature, are reactive chemicals which can seriously corrode materials. For the electronic components themselves, the use of hot air, aeration, and weathering provide the best methods of decontamination for chemical and biological agents. Some decontamination takes place from heat given off by operation of the equipment. For radiation, little can be done

Table 10-3. Protective clothing and equipment for MOPP levels

MOPP	OVERGARMENT	OVERBOOTS	MASK/HOOD	GLOVES
0	Carried	Carried	Carried	Carried
1	Worn, opened or closed based on temperature	Carried	Carried	Carried
2	Same as MOPP 1	Worn	Carried	Carried
3	Same as MOPP 1	Worn	Worn, hooed opened or closed based on temperature	Carried
4	Worn, closed	Worn	Worn, hood closed	Worn

except to reduce radiation levels through aging. Complete decontamination is very difficult, time consuming, and often impossible to accomplish.

c. Electromagnetic pulse and blackout defense.

(1) Protective measures taken for EMP before a nuclear attack are critical to unit survival. Cables, wires, antenna systems, and all metal structures are good electrical conductors. They absorb EMP energy. Material that couples with electromagnetic energy can absorb enough EMP energy to induce voltage and currents. The key to protection is to reduce EMP coupling. The best protection is to have the TACSAT terminals shut down and disconnected prior to a nuclear attack. If not possible, a portion of the equipment may be able to be off the air. Do not forget to take precautions with organic command and control C-E equipment. Protective measures may include ferrous shielding, special voltage limiting devices, and filtering systems built into the equipment. Also, new fiber optic cable systems are EMP resistant and may be used as a replacement for current video and metallic cable systems.

(2) EMP can enter electrical systems through intentional antennas, unintentional antennas, and direct penetration. Intentional antennas are standard radio and radar antennas. An unintentional antenna can be any device (masts, wiring loops, cables, and so forth) that can act as an antenna, even though it is not meant to be one. In direct penetration, internal electronic components act as loop antennas, allowing strong electromagnetic fields to be created inside equipment. See table 10–4 for simple protective measures to use in the absence of built-in protection.

(3) Protective measures for nuclear blackout are extremely limited. Conventional HF, VHF, and UHF techniques for overcoming nuclear blackout are not effective for TACSAT terminals. GMFSC and DSCS controllers will be the only source for assistance. Remember that nuclear blackout lasts for only a limited time, and because it does not affect cable and wire systems, using them might be a simple solution to communicating. However, cable and wire systems are extremely susceptible to EMP energy. Alternate routing can be used to bypass affected regions.

(4) Because TACSAT equipment is so unique, specific details for operating such type under NBC conditions could not be provided here. TACSAT personnel should refer to specific equipment NBC manuals for more detailed instructions.

Table 10-4. EMP protective measures

FOR INTENTIONAL ANTENNAS—

a. Disconnect the antenna.

b. Disconnect all coax, antennas, power sources, cables, and wires from spare equipment.

FOR UNINTENTIONAL ANTENNAS—

a. Keep cable and wire lengths as short as possible. (Energy collected by a cable directly relates to its length.)

b. Bury cables and wires at least 18 inches deep.

c. Never leave cable or wire that is connected to equipment coiled on a reel. (A coil will pick up more EMP than a straight cable run.)

d. Use a common ground for all equipment whenever possible.

e. Ensure antenna guy lines are insulated.

f. Avoid use of commercial sources of power.

FOR DIRECTION PENETRATION—

a. Shield all C-E equipment with iron or steel if available; any metal if not available.

b. Close all enclosure doors, vents, access panels, and ducts.

(Cover with honeycomb metal screens, line with aluminum foil.)